Journal of Algebra **218,** 190–215 (1999)
Article ID jabr.1999.7859, available online at http://www.idealibrary.com on IDEAL®

Character Degrees, Class Sizes, and Normal Subgroups of a Certain Class of p-Groups

Jeffrey M. Riedl

Columbus, Ohio 43210
E-mail: riedl@math.ohio-state.edu

Communicated by George Glauberman

Received July 3, 1997

1. INTRODUCTION

In this paper we investigate a particular class of finite p-groups and their extension groups. These p-groups have appeared before in the literature (see [1]), but the main contribution of this paper is the determination of their character degrees, conjugacy class sizes, and, in some cases, their normal subgroups. These groups are of interest for two main reasons: (i) There are some remarkable connections among the character degrees, the class sizes, and the upper and lower central series of these p-groups; and (ii) these p-groups have some very interesting solvable extension groups, including many examples of odd-order groups possessing properties never before observed in groups of odd order.

Following standard notation, we write $\mathrm{Irr}(G)$ to denote the set of all complex irreducible characters of a finite group G, and we let $\mathrm{cd}(G)$ denote the set of degrees of the members of $\mathrm{Irr}(G)$. We also write $\mathrm{dl}(G)$ to denote the derived length of G. For integers a and b, we denote their greatest common divisor by $\gcd(a, b)$.

Our class of p-groups will be denoted by $P_n(q, e) = P_n$, where q is a prime power, $e \geq 2$, and $n \geq 1$. We impose the conditions $\gcd(e, n!) = 1$ and $\gcd(e, q - 1) = 1$ on the three defining parameters of $P_n(q, e)$. One can see that there are still many ways to choose the three parameters while satisfying these two conditions. We shall see that these groups have order $|P_n(q, e)| = q^{en}$ and nilpotence class n. The upper and lower central series of $P_n(q, e)$ coincide, and so from now on we will often refer to these jointly as the *central series*. Each of the n central factors is naturally isomorphic to

0021-8693/99 $30.00

the additive group of the finite field of order q^e. The derived length of $P_n(q, e)$ is $\lceil \log_2(n+1) \rceil$, which is precisely as large as possible, given the nilpotence class. Some other key information about $P_n(q, e)$ is as follows:

$$\left|\mathrm{Irr}(P_n(q,e))\right| = 1 + \frac{(q^n-1)(q^e-1)}{q-1},$$

$$\text{Conjugacy class sizes: } \left\{ \left(q^{e-1}\right)^i \middle| i = 0, 1, \ldots, n-1 \right\},$$

$$\text{Irreducible character degrees: } \left\{ \left(q^{(e-1)/2}\right)^i \middle| i = 0, 1, \ldots, n-1 \right\}.$$

The sets of class sizes and character degrees of $P_n(q, e)$ are both geometric progressions, and the set of character degrees is equal to the set of square roots of the class sizes. This is a remarkable property and is surely very rare. (In fact we are not aware of any other examples of groups satisfying this property in a nontrivial way.) But even more can be said: The *multiplicities* of the class sizes and of the character degrees match up in the sense just described. More precisely, the number of conjugacy classes of size $(q^{e-1})^i$ is equal to the number of irreducible characters of degree $(q^{(e-1)/2})^i$, for $0 \le i \le n-1$.

There is also a noteworthy relationship between the central series of $P_n(q, e)$ and its class sizes and character degrees. For any nonidentity conjugacy class $\mathscr{K}$ and any nonprincipal irreducible character χ of $P_n(q, e)$, the size of the class and the degree of the character depend only on where that class or character is located with respect to the central series of $P_n(q, e) = P_n$. In particular, for $0 \le i \le n-1$ we have

$$|\mathscr{K}| = \left(q^{e-1}\right)^i \quad \text{if } \mathscr{K} \subseteq \mathbf{Z}_{i+1}(P_n) \text{ and } \quad \mathscr{K} \not\subseteq \mathbf{Z}_i(P_n),$$

$$\chi(1) = \left(q^{(e-1)/2}\right)^i \quad \text{if } \mathbf{Z}_{n-i-1}(P_n) \subseteq \ker(\chi) \text{ and } \quad \mathbf{Z}_{n-i}(P_n) \not\subseteq \ker(\chi).$$

In Section 2 we construct $P_n(q, e)$ as a certain subgroup of the group of units in a truncated skew-polynomial ring R over the finite field $GF(q^e)$, and determine structural information about the group. The group of units in R also contains a cyclic subgroup C of order $c = (q^e - 1)/(q-1)$. The action of C on $P_n(q, e)$ is a Frobenius action, and provides additional information on the structure of $P_n(q, e)$, which plays a crucial role in the later determination of the set of character degrees of $P_n(q, e)$.

In Section 5 we study the solvable extension group P_nCG of order $q^{en}ce$, where G is the Galois group of the field extension $GF(q) \subseteq GF(q^e)$. The

main result of this section is the determination of the set of irreducible character degrees of P_nCG as

$$\mathrm{cd}(P_nCG) = \{1, e\} \cup \left\{c\left(q^{(e-1)/2}\right)^i \middle| i = 0, 1, \ldots, n-1\right\},$$

under the added assumption that e is prime. The group P_nCG has Fitting height 3, derived length $\lceil \log_2(n+1) \rceil + 2$, and satisfies $|\mathrm{cd}(P_nCG)| = n + 2$. One of our two arithmetic conditions (mentioned earlier) on the defining parameters of $P_n(q, e)$ implies that $c = (q^e - 1)/(q - 1)$ is always an odd number, and so the group P_nCG has odd order if and only if the parameters are chosen with e and q both odd. We now highlight some rather special situations which occur in these groups.

For $n = 1$, the group P_1CG is isomorphic to a group of affine semilinear transformations over the field $GF(q^e)$, and it satisfies $\mathrm{dl}(P_1CG) = |\mathrm{cd}(P_1CG)| = 3$. For $n = 2$, we have

$$\mathrm{dl}(P_2CG) = |\mathrm{cd}(P_2CG)| = 4.$$

Not many families of examples of finite solvable groups with 4 character degrees and derived length 4 are known, but we see that the groups P_2CG are indeed such a family, and this family includes for the first time (many) groups of odd order. For $n = 4$, we note that the groups P_4CG provide the first known examples of odd order groups satisfying

$$\mathrm{dl}(P_4CG) = 5, \qquad |\mathrm{cd}(P_4CG)| = 6.$$

Finally, in Section 6 we determine the full set of normal subgroups of $P_n(p, e)$, where we have restricted the prime power q to be a prime p. Our reasons for including this section are: (i) With the knowledge of the class sizes and the character degrees of $P_n(p, e)$, it was possible to find all of its normal subgroups with relatively little extra effort, and (ii) the description which results is interesting and easy to state. For now, however, we wish to say that the only ''hard-to-see'' normal subgroups turn out to be kernels of nonlinear irreducible characters of $P_n(p, e)$.

Note Added in Proof

After the submission of this paper in July 1997, the author became aware of two other very recent papers whose content overlaps most of the content of Sections 2–4 in this paper. Our goal and approach in this paper, however, differ from that of the other authors in their works. We now identify these papers.

A. Hanaki, A condition on the lengths of conjugacy classes and character degrees, *Osaka J. Math.* **33** (1996), 207–216.

A. Hanaki and T. Okuyama, Groups with some combinatorial properties, *Osaka J. Math.* **34** (1997), 337–356.

2. CONSTRUCTION

The first lemma is well known.

LEMMA 2.1. *Let R be a ring (with 1) and let $J = J(R)$ be its Jacobson radical.*

(i) *The coset $1 + J$ is a subgroup of the group of units of R.*

(ii) *If $x \in J^u$ and $y \in J^v$, where u and v are positive integers, then the group commutator $[(1 + x), (1 + y)] \equiv 1 + (xy - yx)$ mod J^{u+v+1}.*

Proof. Part (i) is completely standard. For (ii), note that

$$\begin{aligned}
&\big[(1 + x), (1 + y)\big] - 1 \\
&\quad = (1 + x)^{-1}(1 + y)^{-1}\big((1 + x)(1 + y) - (1 + y)(1 + x)\big) \\
&\quad = (1 + z)(xy - yx) \\
&\quad \equiv xy - yx \qquad \text{mod } J^{u+v+1},
\end{aligned}$$

where we have written $(1 + x)^{-1}(1 + y)^{-1} = 1 + z$ for some element $z \in J$, using (i). ∎

We now construct the truncated skew-polynomial ring R. For a fixed prime power q and an integer $e \geq 2$, let $F = GF(q)$ and let $E = GF(q^e)$. Let $\mathrm{Gal}(E/F) = \langle \sigma \rangle$, where $\sigma\colon \alpha \mapsto \alpha^q$ for $\alpha \in E$. Let $E\{X\}$ denote the skew-polynomial ring in the indeterminate X, with coefficients in E. In other words, the elements of $E\{X\}$ are "polynomials" of the form $\alpha_0 + \alpha_1 X + \cdots + \alpha_k X^k$ with $\alpha_i \in E$, but we do not assume that X commutes with the coefficients. Instead we impose the relation $X\alpha = \alpha^\sigma X$ for $\alpha \in E$. (It is well known that this does define a ring.) Next, fix an integer $n \geq 1$ and note that $X^{n+1}E\{X\} = E\{X\}X^{n+1}$, and that this object is a (two-sided) ideal which we denote by (X^{n+1}). Let $R = E\{X\}/(X^{n+1})$ and let x denote the image of X in R under the natural homomorphism. Every element of R is thus uniquely of the form $\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$, with $\alpha_i \in E$, and $|R| = |E|^{n+1} = q^{e(n+1)}$. Also, $x^{n+1} = 0$ and $x\alpha = \alpha^\sigma x$ for $\alpha \in E$. Note that $xR = Rx$ is a nilpotent ideal and that $R/xR \cong E$. Thus $xR = J(R)$ and we write $xR = J$. We have $J^k = x^k R = Rx^k$ and we see that $J^n \neq 0$ while $J^{n+1} = 0$.

We now define the group $P_n(q, e)$ as the subgroup $1 + J$ (in the situation of Lemma 2.1) of the group $R^\times$ of units in R. In other words,

$$P_n(q, e) = 1 + J = \left\{1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n \,\middle|\, \alpha_i \in E\right\},$$

and so $|P_n(q, e)| = q^{en}$ and $P_n(q, e)$ is a p-group, where p is the unique prime divisor of q. In this paper we shall often write P_n as an abbreviation for $P_n(q, e)$, but it should be understood that the parameters q and e are fixed and essential in the definition of the group. For integers $u \geq 1$,

$$1 + J^u = \left\{1 + \alpha_u x^u + \alpha_{u+1} x^{u+1} + \cdots + \alpha_n x^n \,\middle|\, \alpha_i \in E\right\}$$

is a subgroup, and

$$P_n = 1 + J > 1 + J^2 > \cdots > 1 + J^n > 1 + J^{n+1} = 1.$$

Since each element $s \in 1 + J^u$ is uniquely of the form $s = 1 + \alpha x^u + y$ with $\alpha \in E$ and $y \in J^{u+1}$, we can define the map Ψ_u: $1 + J^u \to E$ by $\Psi_u(s) = \alpha$. In fact, Ψ_u is a homomorphism from $1 + J^u$ onto the additive group of E. To see this, let $s, t \in 1 + J^u$ and write $s \equiv 1 + \alpha x^u$ and $t \equiv 1 + \beta x^u \bmod J^{u+1}$. Then $st \equiv 1 + (\alpha + \beta)x^u \bmod J^{u+1}$ and so

$$\Psi_u(st) = \alpha + \beta = \Psi_u(s) + \Psi_u(t).$$

Note that $\ker(\Psi_u) = 1 + J^{u+1}$ and that $(1 + J^u)/(1 + J^{u+1})$ is naturally isomorphic to the additive group of E.

LEMMA 2.2. *Let u and v be positive integers. Then the group commutator*

$$[1 + J^u, 1 + J^v] \subseteq 1 + J^{u+v}.$$

Furthermore, if $u + v \leq n$ and $s \in 1 + J^u$ and $t \in 1 + J^v$ with $\Psi_u(s) = \alpha$ and $\Psi_v(t) = \beta$, then $\Psi_{u+v}([s, t]) = \alpha\beta^{\sigma^u} - \beta\alpha^{\sigma^v}$.

Proof. We have $s \equiv 1 + \alpha x^u \bmod J^{u+1}$ and $t \equiv 1 + \beta x^v \bmod J^{v+1}$, and so by Lemma 2.1 we have

$$[s, t] \equiv 1 + (\alpha x^u \beta x^v - \beta x^v \alpha x^u) \qquad \bmod J^{u+v+1}.$$

Since $x^u\beta = \beta^{\sigma^u} x^u$ and $x^v\alpha = \alpha^{\sigma^v} x^v$, we have

$$[s, t] \equiv 1 + \left(\alpha\beta^{\sigma^u} - \beta\alpha^{\sigma^v}\right)x^{u+v} \qquad \bmod J^{u+v+1}.$$

Note that $[s,t] \in 1 + J^{u+v}$. In case $u + v \leq n$ this says that $\Psi_{u+v}([s,t]) = \alpha\beta^{\sigma^u} - \beta\alpha^{\sigma^v}$, as claimed. ∎

One immediate consequence of Lemma 2.2 is that the subgroup $1 + J^n$ is central in $P_n(q,e) = 1 + J$, a fact which comes from setting $u = n$ and $v = 1$ in the lemma. Note also that the factor group $P_n/(1 + J^n)$ is naturally isomorphic to the group P_{n-1}. The next two lemmas are well-known facts from elementary number theory, and their proofs are omitted.

LEMMA 2.3. *Let $q > 1$ and $e \geq 1$ be integers. Then* $\gcd(q-1,(q^e-1)/(q-1)) = \gcd(q-1,e)$. *Moreover, if* $\gcd(q-1,e) = 1$, *then* $(q^e-1)/(q-1)$ *is odd.*

LEMMA 2.4. *Let $q > 1$ be an integer, let a and b be positive integers, and write $d = \gcd(a,b)$. Then* $\gcd(q^a-1, q^b-1) = q^d - 1$.

For the remainder of this paper let us assume that all prime divisors of e exceed n (equivalently, $\gcd(e,n!) = 1$). One useful consequence of this assumption is that $\mathrm{Gal}(E/F) = \langle \sigma \rangle = \langle \sigma^u \rangle$ for each integer u such that $1 \leq u \leq n$, since this Galois group is cyclic of order e. From now on we shall also assume that $\gcd(e, q-1) = 1$, which, in view of Lemma 2.3, gives us $\gcd(q-1,(q^e-1)/(q-1)) = 1$. The multiplicative group $E^\times$ is cyclic of order $q^e - 1$, and therefore has a unique subgroup of order $c = (q^e-1)/(q-1)$ (this is an odd number, by Lemma 2.3), which we denote by C. But we also have $F^\times \subseteq E^\times$ with $|F^\times| = q - 1$, and so by coprimality $E^\times = F^\times \times C$. In what follows, we identify C with the subgroup $C \cdot 1$ of the unit group $R^\times$, and we work inside R.

THEOREM 2.5. (i) *$C \subseteq \mathbf{N}_{R^\times}(P_n)$ and $1 + J^u$ is C-invariant for all integers u satisfying $1 \leq u \leq n+1$.*

(ii) *$P_n C$ is a Frobenius group, with kernel P_n and complement C.*

Proof. Let $1 \neq s \in P_n$ and $\gamma \in C$. Then $s = 1 + \alpha x^u + y$ for some unique nonzero element $\alpha \in E$, integer u with $1 \leq u \leq n$, and element $y \in J^{u+1}$. Since $x^u\gamma = \gamma^{\sigma^u}x^u$ we have

$$\gamma^{-1}s\gamma = 1 + \alpha\gamma^{-1}\gamma^{\sigma^u}x^u + \gamma^{-1}y\gamma.$$

We see that $\gamma^{-1}s\gamma \in 1 + J^u$, and this proves (i). If $s = \gamma^{-1}s\gamma$ then this forces $\gamma^{-1}\gamma^{\sigma^u} = 1$ (since $\gamma^{-1}y\gamma \in J^{u+1}$) and so $\gamma \in \mathrm{Fix}(\sigma^u)^\times = \mathrm{Fix}(\sigma)^\times = F^\times$. Hence $\gamma = 1$, since $F^\times \cap C = 1$, and now (ii) is proved. ∎

Since $F \subseteq E$ is a finite-degree extension of fields, we may view E as an e-dimensional vector space over F. For each element $\alpha \in E$, the mapping $\varphi_\alpha\colon E \to E$ defined by $\beta \mapsto \beta\alpha$ is an F-linear operator.

LEMMA 2.6. *Let $\alpha \in E$ and let W be a φ_α-invariant F-subspace of E. Let $F(\alpha)$ denote the subfield of E generated by α over F. Then W is actually an $F(\alpha)$-subspace of E. In particular,* $\dim_F(W) = |F(\alpha):F|\dim_{F(\alpha)}(W)$.

Proof. Note that $F(\alpha) = F[\alpha]$, where $F[\alpha]$ denotes the set of all polynomials in α with coefficients in F. By hypothesis, W is closed under addition and under scalar multiplication by elements of F and by the element α. Hence W is closed under scalar multiplication by all elements of $F(\alpha)$. ∎

Recall that the subgroup $1 + J^n = \{1 + \alpha_n x^n | \alpha_n \in E\}$ is central in $P_n = 1 + J$ and is naturally isomorphic to the additive group of E, and so we may view it as an e-dimensional vector space over F. We now introduce the term *central hyperplane* to refer to any subgroup of $1 + J^n$ that corresponds to an $(e-1)$-dimensional F-subspace of E.

THEOREM 2.7. *The group C regularly permutes the set of all central hyperplanes of $P_n(q, e)$.*

Proof. Given $1 + \alpha x^n \in 1 + J^n$ and $\gamma \in C$, we have $\gamma^{-1}(1 + \alpha x^n)\gamma = 1 + \alpha\gamma^{-1}\gamma^{\sigma^n} x^n$. Let H be a central hyperplane fixed by γ, and write $\epsilon = \gamma^{\sigma^n - 1}$. Viewing H as a φ_ϵ-invariant, $(e-1)$-dimensional F-subspace of E, we apply Lemma 2.6 to H, which tells us that $|F(\gamma^{\sigma^n-1}):F|$ divides $\dim_F(H) = e - 1$. But we also have that $|F(\gamma^{\sigma^n-1}):F|$ divides $|E:F| = e$. Hence we have $F(\gamma^{\sigma^n-1}) = F$, which says that $\gamma^{\sigma^n-1} \in F^\times$. But also $\gamma^{\sigma^n-1} = \gamma^{q^n-1} \in C$, and since $F^\times \cap C = 1$, we have $\gamma^{q^n-1} = 1$, which tells us that $o(\gamma)$ divides $q^n - 1$. But $o(\gamma)$ also divides $q^e - 1$ since $\gamma \in E^\times$, which is cyclic of order $q^e - 1$. Hence $o(\gamma)$ divides $\gcd(q^n - 1, q^e - 1) = q - 1$. But in fact $\gamma \in C$ with $|C| = (q^e - 1)/(q - 1)$, and so $o(\gamma)$ divides $(q^e - 1)/(q - 1)$. Hence $o(\gamma)$ divides $\gcd(q - 1, (q^e - 1)/(q - 1)) = 1$, and so $\gamma = 1$. We have now proved that C permutes the central hyperplanes semiregularly. But the number of central hyperplanes being permuted is $(q^e - 1)/(q - 1) = |C|$, and so the action is regular. ∎

Lemma 2.2 suggests that we study the map $\langle\ ,\ \rangle$: $E \times E \to E$ defined by $\langle \alpha, \beta \rangle = \alpha\beta^{\sigma^u} - \beta\alpha^{\sigma^v}$ for fixed $u, v \geq 1$ with $u + v \leq n$. Note that this map is F-bilinear.

LEMMA 2.8. *If $0 \neq \alpha \in E$, then each of $\langle E, \alpha \rangle$ and $\langle \alpha, E \rangle$ is an F-hyperplane in E.*

Proof. We show that $\langle \alpha, E \rangle$ is an F-hyperplane of E. Consider the F-linear map η_α: $\beta \mapsto \alpha\beta^{q^u} - \beta\alpha^{q^v}$. To show that $\langle \alpha, E \rangle$ is an F-hyperplane of E, it suffices to show that $\ker(\eta_\alpha)$ is one-dimensional as an

F-subspace. Observe that

$$\begin{aligned}\ker(\eta_\alpha) &= \left\{\beta \in E \,\middle|\, \alpha\beta\left(\beta^{q^u-1} - \alpha^{q^v-1}\right) = 0\right\} \\ &= \{0\} \cup \left\{\beta \in E^\times \,\middle|\, \beta^{q^u-1} = \alpha^{q^v-1}\right\}.\end{aligned}$$

Note that if $\delta \in F^\times$ and $\gamma \in C$, then by F-linearity $\ker(\eta_{\delta\gamma}) = \ker(\eta_\gamma)$ and so we may assume that $\alpha \in C$ and so $\alpha^{q^v-1} \in C$. Also, by F-linearity, for $\delta \in F^\times$ and $\gamma \in C$ we see that $\delta\gamma \in \ker(\eta_\alpha)$ if and only if $\gamma \in \ker(\eta_\alpha)$. Hence

$$\left|\left\{\beta \in E^\times \,\middle|\, \beta^{q^u-1} = \alpha^{q^v-1}\right\}\right| = |F^\times| \cdot \left|\left\{\gamma \in C \,\middle|\, \gamma^{q^u-1} = \alpha^{q^v-1}\right\}\right|.$$

Since $1 \le u \le n$ and $\gcd(e, n!) = 1$, we have that $\gcd(u, e) = 1$, and so $\gcd(q^u - 1, q^e - 1) = q - 1$, by Lemma 2.4. Note that $\gcd(q^u - 1, |C|)$ divides $\gcd(q^u - 1, q^e - 1) = q - 1$ and also divides $|C|$. It follows that $\gcd(q^u - 1, |C|) = 1$, since $|C|$ and $q - 1$ are relatively prime.

Thus the mapping $\gamma \mapsto \gamma^{q^u-1}$ is a permutation on C. Hence there exists $\gamma \in C$ unique such that $\gamma^{q^u-1} = \alpha^{q^v-1}$. Therefore $|\ker(\eta_\alpha)| = q$. ∎

LEMMA 2.9. *Let H_1 and H_2 denote a pair of distinct central hyperplanes of P_n. Then their product H_1H_2 is equal to $1 + J^n$.*

Proof. The subgroup H_1H_2 corresponds to the sum of two distinct F-hyperplanes of $1 + J^n$. ∎

Given any integer u such that $1 \le u \le n$ and any nonzero element $\alpha \in E$, we now define the subgroup $S_u(\alpha) = 1 + F\alpha x^u + J^{u+1}$ of $P_n(q, e)$. Note that $1 + J^{u+1} \subseteq S_u(\alpha) \subseteq 1 + J^u$ and that $S_u(\alpha)/(1 + J^{u+1})$ corresponds to the one-dimensional F-subspace of $(1 + J^u)/(1 + J^{u+1})$ generated by α. It is clear that $S_u(\alpha) = S_u(\beta)$ if and only if $\alpha\beta^{-1} \in F$.

THEOREM 2.10. *Let u be an integer such that $1 \le u \le n$. Then the group C regularly permutes the set $\mathcal{S}_u = \{S_u(\alpha) \mid 0 \ne \alpha \in E\}$.*

Proof. Recall from Theorem 2.5 that $1 + J^{u+1}$ and $1 + J^u$ are both invariant under the action of C. For $\gamma \in C$, we see that

$$\gamma^{-1}S_u(\alpha)\gamma = 1 + F\alpha\gamma^{-1}\gamma^{\sigma^u}x^u + J^{u+1} = S_u\left(\alpha\gamma^{-1}\gamma^{\sigma^u}\right).$$

Thus C permutes the members of $\mathcal{S}_u$. Now assume that γ fixes $S_u(\alpha)$. This gives us $\gamma^{-1}\gamma^{\sigma^u} \in F$. But also $\gamma^{-1}\gamma^{\sigma^u} \in C$, and from $F^\times \cap C = 1$ we have $\gamma^{\sigma^u} = \gamma$. Hence $\gamma \in \mathrm{Fix}(\sigma^u) = \mathrm{Fix}(\sigma) = F$, and since $\gamma \in C$, we conclude that $\gamma = 1$, again using the fact that $F^\times \cap C = 1$. This proves that the action of C on $\mathcal{S}_u$ is semiregular. But the members of $\mathcal{S}_u$ are

clearly in one-to-one correspondence with the set of all one-dimensional F-subspaces of E. Hence $|\mathscr{S}_u| = (q^e - 1)/(q - 1) = |C|$, and so the action is in fact regular. ∎

THEOREM 2.11. *Fix any integer u such that $1 \le u \le n - 1$ and define the map $\langle\ ,\ \rangle\colon E \times E \to E$ by $\langle \gamma, \delta \rangle = \gamma\delta^{\sigma^u} - \delta\gamma^{\sigma^{n-u}}$. Let $s, t \in P_n$ such that $s \equiv 1 + \alpha x^u$ and $t \equiv 1 + \beta x^u$ mod J^{u+1}, and such that α and β are both nonzero elements of E. Let T be a subgroup of P_n such that $1 + J^{u+1} \subseteq T \subseteq 1 + J^u$.*

(i) $[S_u(\alpha), 1 + J^{n-u}] = [s, 1 + J^{n-u}] = 1 + \langle \alpha, E \rangle x^n$ *is a central hyperplane.*

(ii) $[S_u(\alpha), 1 + J^{n-u}] = [S_u(\beta), 1 + J^{n-u}]$ *if and only if* $S_u(\alpha) = S_u(\beta)$.

(iii) $[s, 1 + J^{n-u}] = [t, 1 + J^{n-u}]$ *if and only if* $\alpha\beta^{-1} \in F$.

(iv) *Assume $s, t \in T$ and $\alpha\beta^{-1} \notin F$. Then* $[T, 1 + J^{n-u}] = 1 + J^n$.

(v) *If $|T : 1 + J^{u+1}| > q$, then* $[T, 1 + J^{n-u}] = 1 + J^n$.

Proof. For any element $r \in 1 + J^{n-u}$ we may write $r \equiv 1 + \gamma x^{n-u}$ mod J^{n-u+1}. By Lemma 2.2 we have $[s, r] = 1 + (\alpha\gamma^{q^u} - \gamma\alpha^{q^{n-u}})x^n$, so

$$[s, 1 + J^{n-u}] = 1 + \langle \alpha, E \rangle x^n,$$

and of course this is a central hyperplane. Now, by the F-linearity of $\langle\ ,\ \rangle$,

$$[S_n(\alpha), 1 + J^{n-u}] = 1 + \langle F\alpha, E \rangle x^n = 1 + \langle \alpha, E \rangle x^n,$$

proving (i). Now assume that $[S_u(\alpha), 1 + J^{n-u}] = [S_u(\beta), 1 + J^{n-u}]$. By Theorem 2.10 there exists an element $\gamma \in C$ such that $S_u(\alpha)^\gamma = S_u(\beta)$. Hence

$$\begin{aligned}[S_u(\alpha), 1 + J^{n-u}] &= [S_u(\beta), 1 + J^{n-u}] = [S_u(\alpha)^\gamma, 1 + J^{n-u}] \\ &= [S_u(\alpha), 1 + J^{n-u}]^\gamma.\end{aligned}$$

By (i) we see that $[S_u(\alpha), 1 + J^{n-u}]$ is a central hyperplane, and is fixed by $\gamma \in C$. But now Theorem 2.7 forces $\gamma = 1$, and so $S_u(\alpha) = S_u(\beta)$. The reverse implication for (ii) is trivial. Statement (iii) follows easily from (i) and (ii). For (iv), note that from $T \subseteq 1 + J^u$ and Lemma 2.2 we have

$$[T, 1 + J^{n-u}] \subseteq [1 + J^u, 1 + J^{n-u}] \subseteq 1 + J^n.$$

On the other hand, we have $H_1 = [s, 1 + J^{n-u}] \subseteq [T, 1 + J^{n-u}]$ and $H_2 = [t, 1 + J^{n-u}] \subseteq [T, 1 + J^{n-u}]$, and since $\alpha\beta^{-1} \notin F$, (iii) tells us that H_1 and H_2 are distinct central hyperplanes. Now Lemma 2.9 implies that $1 + J^n = H_1 H_2 \subseteq [T, 1 + J^{n-u}]$, and now (iv) is proved. Finally, statement (v) follows easily from (iv). ∎

If u is an integer such that $1 \leq u \leq n - 1$, then by Theorem 2.10 the group C regularly permutes the set $\mathscr{S}_u = \{S_u(\alpha) \mid 0 \neq \alpha \in E\}$, and by Theorem 2.7 the group C regularly permutes the set $\mathscr{H}$ of central hyperplanes of $P_n(q, e)$. The mapping $\theta\colon \mathscr{S}_u \to \mathscr{H}$ defined by $\theta(S) = [S, 1 + J^{n-u}]$, for $S \in \mathscr{S}_u$, is well-defined by Theorem 2.11(i) and is one-to-one by Theorem 2.11(ii). Since $|\mathscr{S}_u| = |C| = |\mathscr{H}|$, this mapping is a bijection. Now since $1 + J^{n-u}$ is a C-invariant subgroup, the group C regularly permutes the set of ordered pairs (S, H) such that $S \in \mathscr{S}_u$ and $H \in \mathscr{H}$ and $H = [S, 1 + J^{n-u}]$.

The final result of this section shows that the normal series $1 + J^u$, for $1 \leq u \leq n + 1$, coincides with the upper and the lower central series of $P_n(q, e)$, and gives the nilpotence class and the derived length of the group.

COROLLARY 2.12. (i) *The ith term* $\mathbf{Z}_i(P_n)$ *in the upper central series of* $P_n(q, e)$ *is* $1 + J^{n-i+1}$, *and so* $P_n(q, e)$ *has nilpotence class* n.

(ii) *If* u *and* v *are positive integers, then* $[1 + J^u, 1 + J^v] = 1 + J^{u+v}$. *In particular,* $1 + J^i$ *is the ith term in the lower central series of* $P_n(q, e)$.

(iii) *The derived length of* $P_n(q, e)$ *is* $\lceil \log_2(n + 1) \rceil$.

Proof. For (i) use induction on i. Since $P_n/(1 + J^n) \cong P_{n-1}$, it suffices to show that $\mathbf{Z}(P_n) = 1 + J^n$. We already know from Lemma 2.2 that $1 + J^n \subseteq \mathbf{Z}(P_n)$. Take any element $s \in P_n$ such that $s \notin 1 + J^n$, and so we have $s \equiv 1 + \alpha_u x^u \bmod J^{u+1}$, for some integer u with $u \leq n - 1$. Now, by Theorem 2.11(i), we see that $[s, 1 + J^{n-u}]$ is a central hyperplane of $P_n(q, e)$, and therefore s is not central in $P_n(q, e)$.

For (ii) we may assume that $u + v = n$, and so $u, v \leq n - 1$. (If necessary, we work in the factor group $P_n/(1 + J^{u+v+1})$.) The fact that $[S_u, S_v] = S_{u+v}$ follows from Theorem 2.11(v), if we set $T = 1 + J^u$ in the notation of that theorem. The statement concerning the lower central series now follows easily, and (ii) is proved.

It follows from (ii) that $1 + J^{2^i}$ is the ith term in the derived series of $P_n(q, e)$, and so the derived length is the smallest positive integer d such that $2^d \geq n + 1$, or, equivalently, $d \geq \log_2(n + 1)$, and this proves (iii). ∎

3. CENTRALIZERS AND CONJUGACY CLASSES OF ELEMENTS OF $P_n(q, e)$

Andrea Previtali was the first to discover a proof of the statements (mentioned in the Introduction) concerning the sizes and locations of the conjugacy classes of $P_n(q, e)$, and we thank him for allowing us to use this result here in this paper. However, the proof that we present here, although inspired by Previtali's proof, is due to Isaacs.

Suppose $r \in J - J^2$. Then $r^i \in J^i - J^{i+1}$, and thus every element $b \in J$ is uniquely of the form $b = \sum \beta_i r^i$, where $\beta_i \in E$ and the sum runs over $1 \leq i \leq n$. In particular, if $a \in J^u - J^{u+1}$, then ar^i lies in $J^{u+i} - J^{u+i+1}$ unless $u + i > n$, in which case, of course, $ar^i = 0$.

LEMMA 3.1. *Let $a \in J^u$ and $\beta \in E$. Then $a\beta \equiv \beta^{\sigma^u} a \bmod J^{u+1}$. In particular, we have $[\beta, a] \equiv (\beta - \beta^{\sigma^u})a \bmod J^{u+1}$.*

Proof. We write $a \equiv \alpha x^u \bmod J^{u+1}$ for $\alpha \in E$. It follows that

$$a\beta \equiv \alpha x^u \beta = \alpha \beta^{\sigma^u} x^u = \beta^{\sigma^u} \alpha x^u \equiv \beta^{\sigma^{ua}} \qquad \bmod J^{u+1}.$$

Thus

$$[\beta, a] = \beta a - a\beta \equiv (\beta - \beta^{\sigma^u})a \qquad \bmod J^{u+1},$$

as desired. ∎

We begin by computing the centralizers in J of certain "good" elements of J, namely elements whose centralizers extend outside of J^2.

LEMMA 3.2. *Let $a \in J^u - J^{u+1}$ and assume that a commutes with some element $r \in J - J^2$. Let $b \in J$ and write b as a polynomial in r, so that*

$$b = \sum_{i=1}^{n} \beta_i r^i,$$

where $\beta_i \in E$. Then b commutes with a if and only if $\beta_i \in F$ for all subscripts i such that $i \leq n - u$. In particular, $|\mathbf{C}_J(a)| = q^{n-u} q^{eu}$.

Proof. Since a centralizes all polynomials in r with coefficients in F, we can assume that some coefficient β_v of b does not lie in F and it is no loss to assume that $\beta_i = 0$ for all subscripts $i < v$. Our goal is to show that b commutes with a if and only if $v > n - u$.

We have

$$[b, a] = \sum_{i=v}^{n} [\beta_i r^i, a] = \sum_{i=v}^{n} [\beta_i, a] r^i,$$

since a commutes with r^i. For notational simplicity, we just write $\beta = \beta_v$.

We have $[\beta, a] \equiv (\beta - \beta^{\sigma^u})a \mod J^{u+1}$, and hence $[b, a] \equiv (\beta - \beta^{\sigma^u})ar^v \mod J^{v+u+1}$. Now σ^u generates $\mathrm{Gal}(E/F)$, and thus $\beta - \beta^{\sigma^u} \neq 0$. If $[b, a] = 0$, therefore, we deduce that $ar^v \equiv 0 \mod J^{v+u+1}$. Since $a \in J^u - J^{u+1}$ and $r^v \in J^v - J^{v+1}$, we see that the only way that ar^v can lie in J^{v+u+1} is to have $v + u > n$. In other words, if $[b, a] = 0$, then $v + u > n$, as desired.

Conversely, if $v > n - u$, then $ar^v = 0$ and $J^{v+u+1} = 0$, and it follows that $[b, a] = 0$. ∎

The next theorem tells us that *all* the elements of J are "good."

THEOREM 3.3. *Let u be an integer with $1 \leq u \leq n$ and let $s = 1 + a \in P_n$, such that $a \in J^u - J^{u+1}$. Then there exists an element $r \in J - J^2$ such that $\mathbf{C}_{P_n}(s) = 1 + Fr + Fr^2 + \cdots + Fr^{n-u} + Er^{n-u+1} + \cdots + Er^n$. Hence $|\mathbf{C}_{P_n}(s)| = q^{n-u}q^{eu}$, and so the conjugacy class of P_n containing s has size $(q^{e-1})^{n-u}$.*

Proof. Since $\mathbf{Z}(P_n) = 1 + J^n$, by Corollary 2.12, we see that the statement of the theorem is true in case $u = n$, and so we may assume that $u < n$. It is clear that $\mathbf{C}_{P_n}(s) = 1 + \mathbf{C}_J(s) = 1 + \mathbf{C}_J(a)$, and so, by Lemma 3.2, it suffices to prove the existence of an element $r \in J - J^2$ that commutes with a. Let X be the set of elements of $J^u - J^{u+1}$ that centralize some element of $J - J^2$. We must show that X is the whole set $J^u - J^{u+1}$, and we do this by counting. Note that $|J^u| = q^{e(n-u+1)}$, so

$$|J^u - J^{u+1}| = q^{e(n-u+1)} - q^{e(n-u)} = q^{e(n-u)}(q^e - 1).$$

Our task, therefore, is to show that $|X| = q^{e(n-u)}(q^e - 1)$.

Given an element $b \in X$, we can find an element $r \in J - J^2$ that commutes with b, and we use Lemma 3.2 to compute that

$$\mathbf{C}_J(b) = Fr + Fr^2 + \cdots + Fr^{n-u} + Er^{n-u+1} + \cdots + Er^n.$$

Hence the number k of elements of $J - J^2$ centralizing b is given by

$$k = |\mathbf{C}_J(b) \cap (J - J^2)| = q^{n-u}q^{eu} - q^{n-u-1}q^{eu} = q^{eu+n-u-1}(q - 1).$$

Now, given $r \in J - J^2$, we see that

$$\mathbf{C}_J(r) = Fr + Fr^2 + \cdots + Fr^{n-1} + Er^n.$$

The number h of elements in $J^u - J^{u+1}$ that centralize r is thus given by

$$h = \left|\mathbf{C}_J(r) \cap (J^u - J^{u+1})\right| = q^{n-u}q^e - q^{n-u-1}q^e = q^{n-u-1+e}(q-1).$$

Finally, we write

$$m = |J - J^2| = q^{ne} - q^{(n-1)e} = q^{ne-e}(q^e - 1).$$

Now mh and $k|X|$ both equal the number of ordered pairs of elements (r, b), where r and b centralize each other, and where $r \in J - J^2$ and $b \in J^u - J^{u+1}$. (Note that all such elements b actually lie in X.) We compute that

$$|X| = \frac{mh}{k} = \frac{q^{ne-e}(q^e-1)q^{n-u-1+e}(q-1)}{q^{eu+n-u-1}(q-1)} = q^{ne-eu}(q^e-1),$$

exactly as required. ∎

COROLLARY 3.4. (i) *The set of sizes of the conjugacy classes of $P_n(q, e)$ is $\{(q^{e-1})^i \mid i = 0, 1, \ldots, n-1\}$.*

(ii) *For each integer u with $1 \le u \le n$, the set $(1 + J^u) - (1 + J^{u+1})$ consists of $q^{n-u}(q^e - 1)$ conjugacy classes of $P_n(q, e)$, each of size $(q^{e-1})^{n-u}$.*

(iii) *$P_n(q, e)$ has $1 + (q^n - 1)(q^e - 1)/(q - 1)$ conjugacy classes.*

Proof. Statement (i) follows immediately from Theorem 3.3. From Theorem 3.3, we see that each conjugacy class of $P_n(q, e)$ contained in the set $(1 + J^u) - (1 + J^{u+1})$ has size $(q^{e-1})^{n-u}$, and, therefore, the number of conjugacy classes of $P_n(q, e)$ in this set is

$$\frac{\left|(1+J^u) - (1+J^{u+1})\right|}{(q^e-1)^{n-u}} = \frac{q^{e(n-u)}(q^e-1)}{(q^{e-1})^{n-u}} = q^{n-u}(q^e-1),$$

and this proves (ii). For (iii), if we let u run from n to 1 in (ii) and include the identity element which is contained in $1 + J^{n+1}$, we compute the cardinality of the set $\mathrm{Cl}(P_n)$ of conjugacy classes of P_n as

$$\begin{aligned}\left|\mathrm{Cl}(P_n)\right| &= 1 + (q^e - 1) + q(q^e - 1) + q^2(q^e - 1) + \cdots + q^{n-1}(q^e - 1)\\ &= 1 + \left(1 + q + q^2 + \cdots + q^{n-1}\right)(q^e - 1)\\ &= 1 + \frac{(q^n - 1)(q^e - 1)}{q - 1},\end{aligned}$$

as desired. ∎

4. THE IRREDUCIBLE CHARACTERS OF $P_n(q, e)$

The following lemma is rather technical and makes no explicit reference to the groups $P_n(q, e)$, but is the key result behind the determination of $\mathrm{cd}(P_n(q, e))$.

LEMMA 4.1. *Let P be a finite p-group with normal series $Z \subseteq N \subseteq A \subseteq B \subseteq P$ such that $[A, B] = 1$ and $A/N \subseteq \mathbf{Z}(P/N)$ and A/N is elementary abelian and $|P : B| \geq p^f$, where $f \geq 1$ is a fixed integer. Let $\lambda \in \mathrm{Irr}(N)$ be linear and P-invariant and let $\chi \in \mathrm{Irr}(P)$ lie over λ, with $Z \not\subseteq \ker(\chi)$. Assume that for every subgroup T such that $B \subseteq T \subseteq P$ and $|T : B| > p^f$, we have $Z \subseteq [T, A]$. Then there exists a subgroup S with $B \subseteq S \subseteq P$ and $|S : B| = p^f$ and there exists $\psi \in \mathrm{Irr}(S)$ such that $\psi^P = \chi$ and $Z \not\subseteq \ker(\psi)$.*

Proof. Induct on $|P : B|$. In case $|P : B| = p^f$ we may take $S = P$ and $\psi = \chi$, which satisfies the conclusion. Now assume that $|P : B| > p^f$. If $A \subseteq \mathbf{Z}(\chi)$, then by setting $T = P$ we obtain

$$Z \subseteq [P, A] \subseteq [P, \mathbf{Z}(\chi)] \subseteq \ker(\chi),$$

which is contrary to our hypotheses. Hence $A \not\subseteq \mathbf{Z}(\chi)$, and since $N \subseteq \mathbf{Z}(\chi)$ and A/N is elementary abelian, there exists a subgroup M_1 such that $N < M_1 \subseteq A$ and $|M_1 : N| = p$ and $M_1 \not\subseteq \mathbf{Z}(\chi)$. Because $A/N \subseteq \mathbf{Z}(P/N)$ we have $M_1 \lhd P$. Take $\lambda_1 \in \mathrm{Irr}(M_1)$ such that λ_1 lies over λ and χ lies over λ_1. The condition $[A, B] = 1$ implies that A is abelian, and this forces λ_1 to be linear. Thus, since $M_1 \not\subseteq \mathbf{Z}(\chi)$, we see that λ_1 is not P-invariant, and so the orbit containing λ_1 in the action of P on $\mathrm{Irr}(M_1)$ has size larger than 1. But since λ is P-invariant, the p irreducible constituents of λ^{M_1}, all of which are linear, and which include λ_1, are a union of P-orbits. These p characters clearly form a single P-orbit.

Let $S_1 = I_P(\lambda_1)$ be the inertia subgroup of λ_1 in P. Then $|P : S_1| = p$, because this index must be equal to the size of the P-orbit containing λ_1. Note that $B \subseteq S_1 \subseteq P$, since B centralizes A. By Theorem 6.11 in [2], we may choose $\chi_1 \in \mathrm{Irr}(S_1)$ lying over λ_1, such that $\chi_1^P = \chi$.

Now if $Z \subseteq \ker(\chi_1)$, it would follow that

$$Z \subseteq \mathrm{core}_P(\ker(\chi_1)) = \ker(\chi_1^P) = \ker(\chi),$$

and this is not the case. Hence $Z \not\subseteq \ker(\chi_1)$. We now apply the inductive hypothesis to the group S_1 with the normal series $Z \subseteq M_1 \subseteq A \subseteq B \subseteq S_1$. Note that

$$p^f < |P : B| = |P : S_1|\,|S_1 : B| = p|S_1 : B|,$$

and so $|S_1 : B| \geq p^f$. We still have $[A, B] = 1$. Clearly $A/M_1 \subseteq \mathbf{Z}(S_1/M_1)$ and A/M_1 is elementary abelian. We have $\lambda_1 \in \mathrm{Irr}(M_1)$, which is linear and S_1-invariant, and also $\chi_1 \in \mathrm{Irr}(S_1)$ lying over λ_1, with $Z \not\subseteq \ker(\chi_1)$. Since $S_1 \subseteq P$ we see that any subgroup T satisfying $B \subseteq T \subseteq S_1$ with $|T : B| > p^f$ also satisfies $B \subseteq T \subseteq P$, and so we still have $Z \subseteq [T, A]$ in this situation. Thus all the hypotheses are satisfied, and by the inductive hypothesis, there exists a subgroup S such that $B \subseteq S \subseteq S_1$ and $|S : B| = p^f$, and there exists $\psi \in \mathrm{Irr}(S)$ such that $\psi^{S_1} = \chi_1$. But since $\chi_1^P = \chi$, we have $\psi^P = \chi$. If $Z \subseteq \ker(\psi)$, then it would follow as before that

$$Z \subseteq \mathrm{core}_P(\psi) = \ker(\psi^P) = \ker(\chi),$$

which is not the case. Hence $Z \not\subseteq \ker(\psi)$. The proof is complete. ∎

LEMMA 4.2. *Let m and n be integers such that $1 \leq m < \frac{n}{2}$ and suppose $\chi \in \mathrm{Irr}(1 + J^m)$ such that $\mathbf{Z}(P_n) \not\subseteq \ker(\chi)$. Then there exists a subgroup S such that $1 + J^{m+1} \subseteq S \subseteq 1 + J^m$ and $|S : 1 + J^{m+1}| = q$, and there exists $\psi \in \mathrm{Irr}(S)$ such that $\psi^{1+J^m} = \chi$. In particular, $\chi(1) = q^{e-1}\psi(1)$ and $\mathbf{Z}(P_n) \not\subseteq \ker(\psi)$.*

Proof. Write $q = p^f$ and recall that $\mathbf{Z}(P_n) = 1 + J^n$. Consider

$$1 + J^n \subseteq 1 + J^{n-m+1} \subseteq 1 + J^{n-m} \subseteq 1 + J^{m+1} \subseteq 1 + J^m.$$

By Lemma 2.2, $1 + J^{n-m+1}$ is central in $1 + J^m$, and so the restriction of χ to $1 + J^{n-m+1}$ is a multiple of a linear character λ. We apply Lemma 4.1 to the above normal series and the characters λ and χ. Note that for every subgroup T satisfying $1 + J^{m+1} \subseteq T \subseteq 1 + J^m$ and $|T : 1 + J^m| > q$, we have $[T, 1 + J^{n-m}] = 1 + J^n$, by Theorem 2.11(v), and so the hypotheses of Lemma 4.1 are indeed satisfied. The fact that $|1 + J^m : S| = q^{e-1}$ gives us $\chi(1) = q^{e-1}\psi(1)$. ∎

LEMMA 4.3. *Let $n = 2m$ be even. Then $\mathrm{cd}(1 + J^m) = \{1, q^{(e-1)/2}\}$, and $1 + J^m$ has exactly q^{me} linear characters and $(q^e - 1)q^{(m-1)e+1}$ irreducible characters of degree $q^{(e-1)/2}$. Moreover, for any irreducible character χ of the group $1 + J^m$, we have $\chi(1) = 1$ if and only if $\mathbf{Z}(P_n) \subseteq \ker(\chi)$.*

Proof. Write $A = 1 + J^m$ and $B = 1 + J^{m+1}$ and recall that $\mathbf{Z}(P_n) = 1 + J^n$. Note that $|A| = q^{(m+1)e}$ and $|B| = q^{me}$, and by Lemma 2.2, B is central in A. For each element $t \in A - B$, we see by Theorem 3.3 that $\mathbf{C}_{P_n}(t) = 1 + Fr + Fr^2 + \cdots + Fr^{n-m} + Er^{n-m+1} + \cdots + Er^n$, for some element $r \in J - J^2$, and so $\mathbf{C}_A(t) = 1 + Fr^{m+1} + Er^{m+2} + \cdots + Er^n$. Therefore $|\mathbf{C}_A(t)| = q^{me+1}$, and so the A-conjugacy class containing t has

size q^{e-1}. Hence the number of A-conjugacy classes in $A - B$ is

$$\frac{|A - B|}{q^{e-1}} = \frac{(q^e - 1)q^{me}}{q^{e-1}} = (q^e - 1)q^{(m-1)e+1},$$

and so $|\mathrm{Irr}(A)| = q^{me} + (q^e - 1)q^{(m-1)e+1}$. By Lemma 2.2, $[A, A] \subseteq \mathbf{Z}(P_n)$, and so $A/\mathbf{Z}(P_n)$ is abelian of order q^{me}. Hence $\mathrm{Irr}(A/\mathbf{Z}(P_n))$ consists of exactly q^{me} linear characters. Now let $\mathscr{T} = \{\chi \in \mathrm{Irr}(A) \mid \mathbf{Z}(P_n) \not\subseteq \ker(\chi)\}$ and let $\chi \in \mathscr{T}$. Since $\mathbf{Z}(\chi)/\ker(\chi)$ is cyclic and $\mathbf{Z}(P_n) \subseteq \mathbf{Z}(\chi)$, it follows that $1 < \mathbf{Z}(P_n)/(\ker(\chi) \cap \mathbf{Z}(P_n))$ is cyclic. But $\mathbf{Z}(P_n)$ is elementary abelian, and this forces $|\mathbf{Z}(P_n) : \ker(\chi) \cap \mathbf{Z}(P_n)| = p$, where p is the unique prime divisor of q. Hence there exists a central hyperplane H such that $H \subseteq \ker(\chi) \cap \mathbf{Z}(P_n)$. By Theorem 2.11 there exists an element $s \in A - B$, for which we may write $s \equiv 1 + \alpha x^m \bmod J^{m+1}$ for some nonzero element $\alpha \in E$, and such that $[s, A] = [S_m(\alpha), A] = H$.

Since $S_m(\alpha) \subseteq A$, this gives us $S_m(\alpha)/H \subseteq \mathbf{Z}(A/H)$. Now we may view $\chi \in \mathrm{Irr}(A/H)$, and by Corollary 2.30 in [2] we have

$$\chi(1)^2 \leq |A/H : \mathbf{Z}(A/H)| \leq |A : S_m(\alpha)| = q^{e-1}.$$

Now because the order of the group A is equal to the sum of the squares of its irreducible character degrees, we have

$$q^{(m+1)e} = |A| = q^{me} + \sum_{\chi \in \mathscr{T}} \chi(1)^2,$$

and so

$$q^{me}(q^e - 1) = \sum_{\chi \in \mathscr{T}} \chi(1)^2 \leq \sum_{\chi \in \mathscr{T}} q^{e-1} = q^{me}(q^e - 1),$$

forcing equality throughout. Therefore $\chi(1) = q^{(e-1)/2}$ for all $\chi \in \mathscr{T}$. ∎

THEOREM 4.4. *Let χ be a nonprincipal irreducible character of $P_n(q, e)$. Then $\chi(1) = (q^{(e-1)/2})^i$ if and only if $\mathbf{Z}_{n-i-1}(P_n) \subseteq \ker(\chi)$ and $\mathbf{Z}_{n-i}(P_n) \not\subseteq \ker(\chi)$. Moreover, $\mathrm{cd}(P_n(q, e)) = \{(q^{(e-1)/2})^i \mid i = 0, 1, \ldots, n - 1\}$, and the number of nonprincipal irreducible characters of $P_n(q, e)$ of degree $(q^{(e-1)/2})^i$ is $q^i(q^e - 1)$, for $0 \leq i \leq n - 1$.*

Proof. We work by induction on n. The case $n = 1$ is clear since P_1 is abelian. In case $n = 2$ it suffices to apply Lemma 4.3 with $n = 2$ and $m = 1$. Now assume that $n > 2$. Write $\mathscr{T} = \{\chi \in \mathrm{Irr}(P_n) \mid \mathbf{Z}(P_n) \not\subseteq \ker(\chi)\}$ and $\mathrm{cd}(\mathscr{T}) = \{\chi(1) \mid \chi \in \mathscr{T}\}$. Note that $\mathrm{cd}(P_n) = \mathrm{cd}(P_n/\mathbf{Z}(P_n)) \cup \mathrm{cd}(\mathscr{T})$.

But we recall that $P_n/\mathbf{Z}(P_n) \cong P_{n-1}$ and so the inductive hypothesis gives

$$\mathrm{cd}(P_n/\mathbf{Z}(P_n)) = \left\{ \left(q^{(e-1)/2}\right)^i \middle| i = 0, 1, \ldots, n-2 \right\},$$

and that $\mathrm{Irr}(P_n \mid \mathbf{Z}(P_n))$ consists of exactly $q^i(q^e - 1)$ nonprincipal irreducible characters of degree $(q^{(e-1)/2})^i$, for $0 \le i \le n-2$. It remains only to determine $\mathrm{cd}(\mathscr{T})$ with multiplicities.

Write $k = \left\lfloor \frac{n-1}{2} \right\rfloor$ and let $Q_i = 1 + J^i$ for $1 \le i \le n$. Choose χ arbitrarily from $\mathscr{T}$. To compute the degree of χ, our approach will be to construct a certain chain of subgroups

$$Q_{k+1} \subseteq S_k \subseteq Q_k \subseteq S_{k-1} \subseteq Q_{k-1} \subseteq \cdots \subseteq S_2 \subseteq Q_2 \subseteq S_1 \subseteq Q_1 = P_n,$$

and to obtain irreducible characters $\chi_i \in \mathrm{Irr}(Q_i)$ and $\psi_i \in \mathrm{Irr}(S_i)$, such that $\psi_i^{Q_i} = \chi_i$ while χ_{i+1} is an irreducible constituent of $(\psi_i)_{Q_{i+1}}$, for $1 \le i \le k$, and such that $\mathbf{Z}(P_n)$ does not lie in the kernel of any of these $2k + 1$ characters.

We now give the construction. First let $\chi_1 = \chi$. It suffices to show how to construct the subgroup S_i and the characters ψ_i and χ_{i+1}, assuming we already have χ_i in hand, where $1 \le i \le k$. We apply Lemma 4.2 to χ_i, taking $m = i$ in the notation of that lemma. This gives us a subgroup S_i and a character $\psi_i \in \mathrm{Irr}(S_i)$, such that $Q_{i+1} \subseteq S_i \subseteq Q_i$ and $|S_i : Q_{i+1}| = q$ and $\psi_i^{Q_i} = \chi_i$ and $\mathbf{Z}(P_n) \not\subseteq \ker(\psi_i)$. Next, we simply choose χ_{i+1} as an irreducible constituent of $(\psi_i)_{Q_{i+1}}$ with the property that $\mathbf{Z}(P_n) \not\subseteq \ker(\chi_{i+1})$.

Because of the relationships among these characters, we have

$$\chi_{i+1}(1) \le \psi_i(1) \qquad \text{and} \qquad q^{e-1}\psi_i(1) = \chi_i(1)$$

for $1 \le i \le k$. Combining these relations, we obtain $q^{e-1}\chi_{i+1}(1) \le \chi_i(1)$. This implies that $q^{(e-1)k}\chi_{k+1}(1) \le \chi_1(1)$, and so $q^{(e-1)k}$ divides $\chi_1(1)$.

We show that in fact $q^{(n-1)(e-1)/2}$ divides $\chi_1(1)$, and from the definition of k, this is clearly true in case n is odd. Assume $n = 2m$ is even. We have $k = \frac{n-2}{2} = m - 1$. Note that $\chi_{k+1} \in \mathrm{Irr}(Q_m)$, and because $\mathbf{Z}(P_n) \not\subseteq \ker(\chi_{k+1})$, Lemma 4.3 applies and tells us that $\chi_{k+1}(1) = q^{(e-1)/2}$. Hence

$$\chi_1(1) \ge q^{(e-1)k} q^{(e-1)/2} = q^{(e-1)((n-2)/2)} q^{(e-1)/2} = q^{((n-1)/2)(e-1)},$$

as desired. Using Corollary 3.4(iii), we find that

$$|\mathscr{T}| = |\mathrm{Irr}(P_n)| - |\mathrm{Irr}(P_{n-1})| = (q^e - 1)q^{n-1}.$$

Therefore, because the order of the group is equal to the sum of the squares of its irreducible character degrees, we have

$$q^{en} = |P_n| = q^{e(n-1)} + \sum_{\chi \in \mathscr{T}} \chi(1)^2,$$

and so

$$(q^e - 1)q^{e(n-1)} = \sum_{\chi \in \mathscr{T}} \chi(1)^2 \geq \sum_{\chi \in \mathscr{T}} q^{(n-1)(e-1)} = (q^e - 1)q^{e(n-1)},$$

and this forces equality throughout. Hence $\chi(1) = q^{(n-1)(e-1)/2}$ for each $\chi \in \mathrm{Irr}(P_n \,|\, \mathbf{Z}(P_n))$, and this completes the proof. ∎

5. ADJOINING THE GALOIS GROUP

In this section we investigate a particular extension group of $P_n(q, e)$ and its character degrees. We have seen that the cyclic group C of order $c = (q^e - 1)/(q - 1)$, which is a multiplicative group consisting of elements of the field E, acts on $P_n(q, e)$ in a Frobenius action. From our knowledge of $\mathrm{cd}(P_n)$ obtained in Section 4, along with Theorem 6.34 in [2], we deduce

$$\mathrm{cd}(P_n C) = \{1\} \cup \left\{ c\left(q^{(e-1)/2}\right)^i \,\middle|\, i = 0, 1, \ldots, n-1 \right\}.$$

It is also not hard to compute the multiplicities of each of the character degrees of $P_n C$, from the knowledge of the multiplicities of the various character degrees of P_n.

Addition and multiplication in the ring R are defined in terms of the operations in the field E and in terms of the field automorphism σ of E. Every automorphism $\tau \in \mathrm{Aut}(E)$ commutes with σ, and therefore τ induces an automorphism of the ring R, and hence an automorphism of the group $R^\times$, defined by letting τ act in its usual way on each of the coefficients of each element of R. The fact that τ and σ commute is needed for the action of τ to respect the identity $x\alpha = \alpha^\sigma x$, for all $\alpha \in E$, which is fundamental to the multiplication in R. In this way, the group $G = \mathrm{Gal}(E/F) = \langle \sigma \rangle$, which is cyclic of order e, acts via automorphisms

on the subgroup

$$P_nC = \left\{\gamma + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n \,\middle|\, \alpha_i \in E,\ \gamma \in C\right\}$$

of $R^\times$. Thus we now have the group P_nCG, which has order $q^{en}ce$.

The main objective of this section is to compute the set of irreducible character degrees of the group P_nCG, under the additional assumption that e is prime, but we shall not assume that e is prime until Theorem 5.5. Since $C \subseteq E^\times$ and $C \cap F^\times = 1$, we see that $G = \mathrm{Gal}(E/F)$ acts without fixed points on C. In case $|G| = e$ is prime, this is a Frobenius action.

As a first step toward computing $\mathrm{cd}(P_nCG)$, we shall determine the number of G-invariant irreducible characters of P_n. Because G is a cyclic group, a theorem of R. Brauer (Theorem 6.32 in [2]) tells us that the number of G-fixed conjugacy classes of P_n is equal to the number of G-fixed irreducible characters of P_n, and so we shall count the former to obtain the latter. The first lemma of this section tells us that any pair of elements of $P_n(q, e)$ that are conjugate inside $P_n(q, e)$ share the same lowest-order nonzero nonconstant coefficient, a fact which will be useful in determining which conjugacy classes of $P_n(q, e)$ are G-invariant.

LEMMA 5.1. *Let $1 \neq s \in P_n(q, e)$ and write $s \equiv 1 + \alpha x^u \bmod J^{u+1}$, for nonzero $\alpha \in E$. Then every conjugate t of s in $P_n(q, e)$ satisfies $t \equiv 1 + \alpha x^u \bmod J^{u+1}$.*

Proof. By Corollary 2.12, s is central in $P_n(q, e)$ modulo $1 + J^{u+1}$, and so any conjugate of s is unchanged modulo $1 + J^{u+1}$. ∎

Recall from Section 2 the definition of the groups $S_u(\alpha) = 1 + F\alpha x^u + J^{u+1}$, where $1 \leq u \leq n$ and $0 \neq \alpha \in E$. Because it is central in $P_n(q, e)$ modulo the normal subgroup $1 + J^{u+1}$, we see that $S_u(\alpha)$ is normal in $P_n(q, e)$. Thus $S_u(1) = 1 + Fx^u + J^{u+1}$ is a normal G-invariant subgroup of $P_n(q, e)$, and it satisfies the conditions $1 + J^{u+1} \subseteq S_u(1) \subseteq 1 + J^u$ and $|S_u(1) : 1 + J^{u+1}| = q$ and $|1 + J^u : S_u(1)| = q^{e-1}$. For all integers u such that $1 \leq u \leq n$, therefore, we see that each of $(1 + J^u) - S_u(1)$ and $S_u(1) - (1 + J^{u+1})$ is a union of P_n-conjugacy classes, and because in addition all of these normal subgroups are union of P_n-conjugacy classes, and because in addition all of these normal subgroups are G-invariant, each of $(1 + J^u) - S_u(1)$ and $S_u(1) - (1 + J^{u+1})$ is a union of G-orbits in its action on the set of conjugacy classes of P_n.

The next two lemmas describe exactly which conjugacy classes of elements of $P_n(q, e)$ are G-invariant, and this will allow us to count these G-invariant classes easily.

LEMMA 5.2. *Let $\mathscr{K}$ be a conjugacy class of elements of P_n, such that $\mathscr{K} \subseteq (1 + J^u) - S_u(1)$ for some integer u such that $1 \leq u \leq n$. Then $\mathscr{K}$ is not fixed by G.*

Proof. Take an element $s \in \mathscr{K}$ and write $s = 1 + \alpha x^u + y$, where $y \in J^{u+1}$ and $\alpha \in E - F$. If $\mathscr{K}$ were fixed by $G = \langle \sigma \rangle$, it would then follow that $s^\sigma = 1 + \alpha^\sigma x^u + y^\sigma \in \mathscr{K}$, with $y^\sigma \in J^{u+1}$. But since $\alpha^\sigma \neq \alpha$, this would contradict Lemma 5.1. ∎

LEMMA 5.3. *Let $\mathscr{K}$ be a conjugacy class of elements of $P_n(q, e)$, such that $\mathscr{K} \subseteq S_u(1) - (1 + J^{u+1})$ for some integer u such that $1 \leq u \leq n$. Then $\mathscr{K}$ is fixed by G.*

Proof. Take any element $s \in \mathscr{K}$. Since $G = \langle \sigma \rangle = \langle \sigma^u \rangle$, showing that the elements s and s^{σ^u} are conjugate in $P_n(q, e)$ would be sufficient for proving that $\mathscr{K}$ is G-invariant. Let us write

$$s = 1 + \alpha_u x^u + \cdots + \alpha_n x^n = 1 + ax^u,$$

where $a = \alpha_u + \alpha_{u+1} x + \cdots + \alpha_n x^{n-u}$. By hypothesis we have $0 \neq \alpha_u \in F$, and so α_u is fixed by the field automorphism σ. Note that

$$s^{\sigma^u} = 1 + a^{\sigma^u} x^u = 1 + x^u a.$$

We seek an element $t = 1 + b \in P_n$ that conjugates s to s^{σ^u}. Since

$$st = (1 + ax^u)(1 + b) = 1 + b + (a + ab^{\sigma^u}) x^u$$

and

$$ts^{\sigma^u} = (1 + b)(1 + a^{\sigma^u} x^u) = 1 + b + (a^{\sigma^u} + ba^{\sigma^u}) x^u,$$

it suffices to produce an element $b \in J$ such that $a + ab^{\sigma^u} = a^{\sigma^u} + ba^{\sigma^u}$. We take $b = \alpha_u^{-1}(a - \alpha_u)$, and from this we have

$$a + ab^{\sigma^u} = a + a\alpha_u^{-1}(a - \alpha_u)^{\sigma^u} = a + \alpha_u^{-1} aa^{\sigma^u} - a = \alpha_u^{-1} aa^{\sigma^u}$$

and

$$a^{\sigma^u} + ba^{\sigma^u} = a^{\sigma^u} + \alpha_u^{-1}(a - \alpha_u) a^{\sigma^u} = a^{\sigma^u} + \alpha_u^{-1} aa^{\sigma^u} - a^{\sigma^u} = \alpha_u^{-1} aa^{\sigma^u}.$$

These two quantities are equal, as desired. ∎

THEOREM 5.4. *$P_n(q, e)$ has q^n G-invariant irreducible characters.*

Proof. Let $\mathrm{Irr}_G(P_n)$ and $\mathrm{Cl}_G(P_n)$ respectively denote the set of G-invariant irreducible characters and the set of G-invariant conjugacy classes

of the group P_n. By Corollary 3.4, if $\mathscr{K}$ is a nonidentity conjugacy class of P_n such that $\mathscr{K} \subseteq (1 + J^u) - (1 + J^{u+1})$, then $|\mathscr{K}| = q^{(n-u)(e-1)}$ for $1 \leq u \leq n$. But $|S_u(1) : 1 + J^{u+1}| = q^{(n-u)e}(q-1)$, and so the number of conjugacy classes of P_n that are contained in $S_u(1) - (1 + J^{u+1})$ is

$$\frac{q^{(n-u)e}(q-1)}{q^{(n-u)(e-1)}} = q^{n-u}(q-1),$$

and each of these classes is G-fixed, by Lemma 5.3. Including the identity element, we compute the number of G-fixed conjugacy classes of P_n as

$$\begin{aligned}&\left|\mathrm{Cl}_G(P_n)\right| \\ &\quad = 1 + \sum_{u=1}^{n} q^{n-u}(q-1) = 1 + (q-1)\left(q^{n-1} + \cdots + q + 1\right) = q^n.\end{aligned}$$

Finally, because G is cyclic, Theorem 6.32 in [2] tells us that $|\mathrm{Irr}_G(P_n)| = |\mathrm{Cl}_G(P_n)| = q^n$, as desired. ∎

At this point we would like to mention that in the special case where the characteristic p of the field E does not divide e, a much simpler proof of Theorem 5.4 is available, and the computations in the proof of Theorem 5.3 can be avoided. This simpler proof is as follows. Since G acts on P_n with $\gcd(|G|, |P_n|) = 1$, the number of G-invariant irreducible characters of P_n is equal to the number of irreducible characters of the group of G-fixed elements of P_n. Next observe that

$$\mathbf{C}_{P_n}(G) = \left\{1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n \,\middle|\, \alpha_i \in F\right\}$$

is abelian of order q^n, and so $\left|\mathrm{Irr}_G(P_n)\right| = \left|\mathrm{Irr}\left(\mathbf{C}_{P_n}(G)\right)\right| = \left|\mathbf{C}_{P_n}(G)\right| = q^n$.

In the following main result for this section, we need to make the additional assumption that e is prime.

THEOREM 5.5. *Let e be prime. Then* $\mathrm{cd}(P_nCG) = \{1, e\} \cup \{c(q^{(e-1)/2})^i \mid i = 0, 1, \ldots, n-1\}$. *Also, every nonlinear irreducible character of P_nC extends to P_nCG.*

Proof. Since CG is a Frobenius group we see that $\mathrm{cd}(P_nCG/P_n) = \mathrm{cd}(CG) = \{1, e\}$. Now it remains to consider the irreducible characters of P_nCG lying over the nonprincipal characters of P_n. We know that P_nC is a

normal subgroup of prime index e in P_nCG, and thus each irreducible character of P_nCG either restricts irreducibly to P_nC or its restriction is a sum of e distinct characters. It thus suffices to show that G fixes each irreducible character of P_nC whose kernel does not contain P_n, and for this it is enough to show that each C-orbit of nonprincipal characters of P_n contains a chracter fixed by G.

Let Δ denote the set of all nonprincipal G-invariant irreducible characters of P_n. Note that $|\Delta| = q^n - 1$, by Theorem 5.4. Observe that the $|C| = c$ subsets

$$\Delta^\gamma = \{ \chi^\gamma \mid \chi \in \Delta\} \qquad \text{for } \gamma \in C$$

are pairwise disjoint. To see this, note that if $\psi \in \Delta^\gamma \cap \Delta^\delta$ for elements γ and δ in C, then it follows that P_nG^γ and P_nG^δ are contained in $I = I_{P_nCG}(\psi)$. But since $I \cap P_nC = P_n$, we have $|P_nCG : I| \geq c$, and this forces $P_nG^\gamma = I = P_nG^\delta$, which implies $G^\gamma = G^\delta$, and so $\gamma = \delta$, since G is a Frobenius comlement in CG.

By Corollary 3.4(iii), we have $|\mathrm{Irr}(P_n) - \{1_{P_n}\}| = (q^n - 1)(q^e - 1)/(q - 1) = (q^n - 1)c$, and so by counting we see that

$$\mathrm{Irr}(P_n) - \{1_{P_n}\} = \bigcup_{\gamma \in C} \Delta^\gamma,$$

where the union is disjoint. Hence the C-conjugates of the set Δ cover $\mathrm{Irr}(P_n) - \{1_{P_n}\}$, as desired. ∎

6. THE NORMAL SUBGROUPS OF $P_n(p, e)$

It is not often that one can describe all the normal subgroups of a large p-group. We accomplish this for the group $P_n(q, e)$, however, in the special case where the prime power $q = p^f$ is actually a prime. (To emphasize this, we shall use p rather than q in the notation throughout this section.) Of course we continue to assume the conditions $\gcd(e, n!) = 1$ and $\gcd(e, p - 1) = 1$. Which normal subgroups of $P_n(p, e)$ are evident to us, with our knowledge up to this point of the group's structure? We know its upper/lower central series and we know that each of these central factors is elementary abelian of order p^e, and this already provides us with the knowledge of many normal subgroups. Every subgroup H of $P_n(p, e)$ such that $1 + J^{u+1} \subseteq H \subseteq 1 + J^u$, for some $1 \leq u \leq n$, is normal in $P_n(p, e)$, and these normal subgroups will be called *tame*, because they are easy to see. The tame normal subgroups are plentiful in $P_n(p, e)$, and counting these amounts to counting the total number of subspaces in the e-dimensional vector space over the field of order p, for each of the n central factors of $P_n(p, e)$. It is clear that all the normal subgroups of $P_1(p, e)$ are

tame. Any normal subgroups of $P_n(p,e)$ which are not tame will be called *wild*. The surprising fact is that the only wild normal subgroups of $P_n(p,e)$ turn out to be kernels of nonlinear irreducible characters of the group.

The first lemma of this section provides basic information concerning the exponent of the group $P_n(p,e)$. Analogues of both statements in this lemma hold in the more general situation where q is a prime power that might not be prime.

LEMMA 6.1. (i) *If $p \geq n+1$, then the group $P_n(p,e)$ has exponent p.*

(ii) *Let m be an integer such that $\frac{n}{2} < m \leq n$. Then the subgroup $1+J^m$ of $P_n(p,e)$ is elementary abelian.*

Proof. (i) An arbitrary element of $P_n(p,e)$ has the form $1+xa$, for some element $a \in R$. Since the ring R has characteristic p, we have

$$(1+xa)^p = 1 + (xa)^p \in 1 + J^p \subseteq 1 + J^{n+1} = 1,$$

as desired.

(ii) Given elements $s = 1 + \alpha_m x^m + \cdots + \alpha_n x^n$ and $t = 1 + \beta_m x^m + \cdots + \beta_n x^n$ in $1+J^m$ with coefficients in the field E, their product is

$$st = 1 + (\alpha_m + \beta_m)x^m + \cdots + (\alpha_n + \beta_n)x^n + \text{terms of degree larger than } n,$$

since $2m \geq n+1$. But the terms of degree larger than n vanish (because $x^{n+1} = 0$), and so multiplication in the subgroup $1+J^m$ amounts to adding the corresponding nonconstant coefficients. Now the fact that the additive group of the field E is elementary abelian forces the subgroup $1+J^m$ to be elementary abelian. ∎

Theorem 4.4 says that $\mathrm{cd}(P_n(p,e)) = \{(p^{(e-1)/2})^i \mid i = 0,1,\ldots,n-1\}$. The following result proves the existence (assuming $n \geq 2$) of wild normal subgroups of $P_n(p,e)$, provided that n and p are not both equal to 2.

THOREM 6.2. *Let $n \geq 2$ and let $\chi \in \mathrm{Irr}(P_n(p,e))$ be nonlinear. Then $\ker(\chi)$ is a wild subgroup of $P_n(p,e)$, unless $p = 2$ and $\chi(1) = 2^{(e-1)/2}$.*

Proof. In view of Theorem 4.4, since χ is nonlinear, we see that $\chi(1) = (p^{(e-1)/2})^i$ for some integer i such that $1 \leq i \leq n-1$, and that $\mathbf{Z}_{n-i-1}(P_n) \subseteq \ker(\chi)$, while $\mathbf{Z}_{n-i}(P_n) \not\subseteq \ker(\chi)$. We work in the factor group $P_n/\mathbf{Z}_{n-i-1}(P_n)$ (which is naturally isomorphic to P_{i+1}), and so (possibly after renaming n) we may assume that $i = n-1$, and this gives us $\chi(1) = (p^{(e-1)/2})^{n-1}$ and $\mathbf{Z}(P_n) \not\subseteq \ker(\chi)$.

To show that $\ker(\chi)$ is wild, it suffices to show that $\ker(\chi) \not\subseteq \mathbf{Z}(P_n)$ (since $1 + J^n = \mathbf{Z}(P_n)$), and we prove this by contradiction. Suppose that $\ker(\chi) \subseteq \mathbf{Z}(P_n)$. This inclusion cannot be an equality and so we have $\ker(\chi) < \mathbf{Z}(P_n) \subseteq \mathbf{Z}(\chi)$. Because $\mathbf{Z}(\chi)/\ker(\chi)$ is cyclic and $\mathbf{Z}(P_n)$ is elementary abelian, we see that $\mathbf{Z}(P_n)/\ker(\chi)$ is cyclic of order p, and thus $\ker(\chi)$ is a central hyperplane of P_n (because $q = p$). Hence by Lemma 2.11 there exists $S/\mathbf{Z}(P_n) \subseteq \mathbf{Z}_2(P_n)/\mathbf{Z}(P_n)$, such that $|S : \mathbf{Z}(P_n)| = p$ and $[P_n, S] = \ker(\chi)$. Therefore $S/\ker(\chi) \subseteq \mathbf{Z}(P_n/\ker(\chi)) = \mathbf{Z}(\chi)/\ker(\chi)$, and so $S/\ker(\chi)$ is cyclic of order p^2 with $S \subseteq \mathbf{Z}_2(P_n)$. But if $n \geq 3$, we know from Lemma 6.1(ii) that $\mathbf{Z}_2(P_n) = 1 + J^{n-1}$ is elementary abelian, and this would contradict what we know about S. Hence we may assume that $n = 2$. If $p \geq 3$, then $p \geq n + 1$, and Lemma 6.1(i) implies that P_2 has exponent p, again contradicting the above information about S. Therefore $n = p = 2$ and $\chi(1) = 2^{(e-1)/2}$. ∎

Next we describe the kernels of irreducible characters of degree $2^{(e-1)/2}$.

THEOREM 6.3. *Let* $\chi \in \mathrm{Irr}(P_n(2, e))$ *such that* $\chi(1) = 2^{(e-1)/2}$. *Then* $\ker(\chi)$ *is a tame subgroup of* $P_n(2, e)$.

Proof. By Theorem 4.4 we see that $\mathbf{Z}_{n-2}(P_n) \subseteq \ker(\chi)$, and so we may assume that $n = 2$. We will show that $\ker(\chi)$ is a central hyperplane of $P_2(2, e)$, and this will be sufficient for proving the theorem. Take the element $s = 1 + x \in P_2$ and let $S = \langle s, \mathbf{Z}(P_2)\rangle$. Note that $|S| = 2^{e+1}$. Recall from Theorem 2.11(i) that

$$[P_2, S] = [P_2, s] = \left\{1 + (\alpha^2 - \alpha)x^2 \,\middle|\, \alpha \in E = GF(2^e)\right\} = H$$

is a central hyperplane. Note that $S/H \subseteq \mathbf{Z}(P_2/H)$, and from Theorem 2.11(v) it follows that $S/H = \mathbf{Z}(P_2/H)$.

We claim that S/H is a cyclic group (which distinguishes this case from that of Theorem 6.2). Since $|S : H| = 4$, we can prove this by showing that $s^2 = (1 + x)(1 + x) = 1 + x^2 \notin H$, and for this it is enough to show that the equation $1 = \alpha^2 - \alpha$ has no solution in $GF(2^e)$. But any solution α would satisfy the polynomial $f(X) = X^2 + X + 1$, which is irreducible over the prime subfield $F = GF(2)$, and would give us the situation $F \subseteq F(\alpha) \subseteq E$ with $|F(\alpha) : F| = 2$ dividing $|E : F| = e$, and this cannot happen because e is odd. Hence S/H is cyclic, as claimed.

Recall from the comments following Theorem 2.11 that the group C transitively permutes the set of ordered pairs (S, H) where $\mathbf{Z}(P_2) \subseteq S \subseteq P_2$ with $|S : \mathbf{Z}(P_2)| = 2$ and $H = [P_2, S]$ is the corresponding central hyperplane. Therefore $S/H = \mathbf{Z}(P_2/H)$ is cyclic of order 4 for all such pairs. Since $\ker(\chi) \cap \mathbf{Z}(P_2)$ is a central hyperplane, we may assume that $\ker(\chi)$

$\cap \mathbf{Z}(P_2) = H$. Because $\mathbf{Z}(P_2/H)$ is cyclic, P_2/H has a unique minimal normal subgroup, and this must be $(P_2/H)' = \mathbf{Z}(P_2)/H$. Therefore every nonlinear irreducible character of P_2/H is faithful, and so, because χ is nonlinear with $H \subseteq \ker(\chi)$, we conclude that $H = \ker(\chi)$. ∎

We now know that kernels of nonlinear irreducible characters of $P_n(p, e)$ provide us with a source of wild subgroups of $P_n(p, e)$, assuming that $n \geq 2$ and that p and n are not both equal to 2. The following theorem shows that these are the *only* wild subgroups of $P_n(p, e)$, and in effect completes our search for the full set of normal subgroups of $P_n(p, e)$.

THEOREM 6.4. *Let $n \geq 2$ and let W be a wild subgroup of $P_n(p, e)$. Then $W = \ker(\chi)$ for some nonlinear $\chi \in \mathrm{Irr}(P_n(p, e))$.*

Proof. We choose i maximal such that $\mathbf{Z}_i(P_n) \subseteq W$, and we work in the factor group $P_n/\mathbf{Z}_i(P_n)$. Thus (possibly after renaming n) we may assume that $\mathbf{Z}(P_n) \not\subseteq W$. Hence $1 < W\mathbf{Z}(P_n)/W \lhd P_n/W$, and so there exists $\chi \in \mathrm{Irr}(P_n/W)$ such that $\mathbf{Z}(P_n) \not\subseteq \ker(\chi)$. Theorem 4.4 now asserts that $\chi(1) = p^{(n-1)(e-1)/2} > 1$. Write $H = \mathbf{Z}(P_n) \cap \ker(\chi)$ and note that $H < \mathbf{Z}(P_n)$. Since $\mathbf{Z}(P_n)/H$ is isomorphic to a subgroup of the cyclic group $\mathbf{Z}(\chi)/\ker(\chi)$ and since $\mathbf{Z}(P_n)$ itself is elementary abelian, we see that $|\mathbf{Z}(P_n) : H| = p$, which says that H is a central hyperplane of P_n.

We now show that $\mathbf{Z}(\chi) \subseteq \mathbf{Z}_2(P_n)$. Assuming this is false, $\mathbf{Z}(\chi)$ contains an element $s \notin \mathbf{Z}_2(P_n) = 1 + J^{n-1}$, and if we let $\mathscr{K}$ denote the conjugacy class of P_n containing s, then Corollary 3.4(ii) implies that $|\mathscr{K}| > p^{2e-2}$. Since $\mathbf{Z}(\chi) \lhd P_n$ we have $\{1\} \cup \mathscr{K} \subseteq \mathbf{Z}(\chi)$, and this implies that $p^{2e-1} \leq |\mathbf{Z}(\chi)|$. Define m by $|\mathbf{Z}(\chi)| = p^m$. Then by Corollary 2.30 in [2], we have

$$p^{(n-1)(e-1)} = \chi(1)^2 \leq |P_n : \mathbf{Z}(\chi)| = p^{ne-m}.$$

Hence $(n-1)(e-1) \leq ne - m$ and this gives us $m \leq n + e - 1$. Thus

$$p^{2e-1} \leq |\mathbf{Z}(\chi)| = p^m \leq p^{n+e-1},$$

and so we have $2e - 1 \leq n + e - 1$, and this implies that $e \leq n$. But the conditions $\gcd(e, n!) = 1$ and $e \geq 2$ together imply that $n < e$, and this is a contradiction and proves that $\mathbf{Z}(\chi) \subseteq \mathbf{Z}_2(P_n)$, as desired.

Next we show that $\mathbf{Z}(\chi)/H \subseteq \mathbf{Z}(P_n/H)$. Since $\mathbf{Z}(\chi) \subseteq \mathbf{Z}_2(P_n)$, while the upper and lower central series of P_n coincide, it follows that

$$[P_n, \mathbf{Z}(\chi)] \subseteq [P_n, \mathbf{Z}_2(P_n)] = \mathbf{Z}(P_n),$$

and because $[P_n, \mathbf{Z}(\chi)] \subseteq \ker(\chi)$ we see that

$$\big[P_n, \mathbf{Z}(\chi)\big] \subseteq \ker(\chi) \cap \mathbf{Z}(P_n) = H,$$

as desired.

We now determine $\mathbf{Z}(P_n/H)$. Since $H \subseteq \mathbf{Z}(P_n)$, we have $\mathbf{Z}(P_n/H) \subseteq \mathbf{Z}_2(P_n)/H$. In view of the comments following Theorem 2.11, there exists a unique subgroup S such that $\mathbf{Z}(P_n) \subseteq S \subseteq \mathbf{Z}_2(P_n)$ and $|S : \mathbf{Z}(P_n)| = p$ and $[S, P_n] = H$. Moreover, for each element $t \in \mathbf{Z}_2(P_n) - S$, Theorem 2.11(v) asserts that $[\langle S, t\rangle, P_n] = \mathbf{Z}(P_n)$, and so we conclude that $\mathbf{Z}(P_n/H) = S/H$.

We now have $W \subseteq \ker(\chi) < \mathbf{Z}(\chi) \subseteq S$ and $|S| = p^{e+1}$. To finish the proof, it suffices to show that $|W| \geq p^e$. Since W is wild, we have $W \notin \mathbf{Z}(P_n)$, and so W contains a noncentral element r of P_n. If we let $\mathscr{L}$ denote the conjugacy class of P_n containing r, we see by Corollary 3.4 that $|\mathscr{L}| \geq p^{e-1}$. Since W is normal we have $\{1\} \cup \mathscr{L} \subseteq W$, and this forces $|W| \geq p^e$, as desired. ∎

ACKNOWLEDGMENTS

I thank Professor I. M. Isaacs for the many helpful ideas and suggestions which he contributed during the writing of this paper. I also acknowledge the GAANN fellowship which supported me during the spring semester of 1997, while I worked on this paper.

REFERENCES

1. I. M. Isaacs, Coprime group actions fixing all nonlinear irreducible characters, *Canad. J. Math.* **41** (1989), 68–82.
2. I. M. Isaacs, "Character Theory of Finite Groups," Dover, New York, 1994.